Mainframe Security:

The somewhat locked candy shop

Table of contents

Executive summary

The mainframe computer? Didn't companies replace them during Y2K because they were going to have to recode everything? Isn't the mainframe dead?

It's true that many new systems admins and IT administrators thought x86 systems were the only servers to power large data centers and the Cloud. But the truth is, the mainframe never went away. Mainframe computers simply kept evolving and delivering more and more performance. The mainframe was and is critical to commercial databases, transaction servers and applications that require high reliability, scalability, compatibility and speed. In fact, mainframes handle 30 billion business transactions every single day—and that number is only expected to grow[1].

However, companies face challenges ensuring their mainframes are secure. With IT resources stretched and criminal attacks on the rise, CIOs and CISOs need to make sure their mainframes are locked down. Previously thought unhackable, several hackers have proven that criminal attackers can access mainframes and often easily escalate privileges to gain control of sensitive data.

There are several ways companies can manage mainframe security—from manual penetration testing to hiring outside teams of hackers who run continuous security testing that identifies vulnerabilities, and then methodically working through any exploitable mainframe issues. The reality is that even though mainframes are isolated with their own security controls, and there is limited mainframe hacking expertise, compromises can happen. Continuous testing services can help expose vulnerabilities criminal attackers could potentially leverage to steal sensitive corporate and customer information.

X-Force® Red, an autonomous team of hackers within IBM Security can help. With X-Force Red's attacker mentality, the team can uncover, prioritize and help fix security vulnerabilities across the IT infrastructure, doing what criminal attackers can do, with the goal of helping security leaders harden their defenses to protect their most important assets.

The unhackable mainframe?

Today's mainframes are powerful, but not as large as their old nickname, Big Iron, implies. In fact, many mainframes can slide into any data center, fitting in the space of 2 floor tiles. What makes a mainframe is not its size, but how it is designed to perform—which is to quickly process huge numbers of transactions for banks, insurance companies, and yes, even for that online retailer who sells books and groceries. Mainframes are called Big Iron for a reason—and it's not because they're old dinosaurs.

Here are some stats to consider:

64% **of responding enterprises run more than half of their critical applications on a mainframe.[2]**

99.999 **Percentage of uptime, or less than 1 minute of unplanned downtime per server per year.[3]**

1,500 **The number of x86 servers the can be consolidated onto a single mainframe.[4]**

Decades **What the mainframe's *Mean Time Between Failure* is measured in.[5]**

Except, there's one tiny problem: while the mainframe is reliable, fast, and efficient, it has also now been proven to be hackable.

There was a misconception in the industry that mainframes were unhackable. That was because lack of exposure and experience limited who could attack mainframes. Typically, the machines are located in secure data centers, with limited physical access and their own stringent security controls. There also used to be many layers between the mainframe hardware and connection to the Internet. Now, however, many mainframes are connected directly to the Internet with no layers in between, providing a more direct path for attackers to potentially compromise the machines.

In 2015, two researchers, whose jobs as IT professionals at major financial institutions required them to ensure their organizations' data and systems are secured, demonstrated various back ways to compromise mainframes. Phil Young, also known as Soldier of Fortran, and Chad Rikansrud, also known as Bigendian Smalls, hacked into a mainframe using bypass techniques, or privilege escalation, by using compromised user credentials. Their research showed how attackers could escalate privileges once the mainframe is compromised, giving them full access to their target's crown jewels. In the past, mainframe communications often lacked encryption. Login credentials were sent in the clear, enabling an attacker to access all credentials and log in as a legitimate user undetected. Also, the communication going back and forth between virtual hosts and over the network was de facto unencrypted. Virtual host communications are internal-only, which is why there tends to be no authentication nor encryption on it. However, if there's an insider who wants to attack a mainframe, the messaging can provide useful information.

And according to Verizon's 2019 Data Breach Investigation Report,

40%

of insider attackers are disgruntled employees—and the type of attack most often executed is privilege abuse.[5]

Configuring the keys to the kingdom

Setting up mainframes can be a complex process. In some cases, mainframes may be misconfigured at the start with security flaws unknowingly created during the configuration process. There can also be security flaws created during the set-up of permissions for libraries. Libraries are modules for coding. They call into the code and should only be accessed by people who have the highest level of permission. Yet, often the permissions are not set at the right levels, meaning people who shouldn't have access to the libraries can abuse those right.

Access rights for "Super Users" can also be a problem. Super Users can see and run anything on a mainframe; it's the highest level of access and gives the user the keys to the kingdom. If more people than necessary are granted super user access rights, risk becomes elevated since more people are able to control what runs on the mainframe.

Part of the challenge also lies with resources. Often IT departments are run lean. According to a 2018 Forrester report, enterprises have lost an average of 23 percent of specialized mainframe staff in the last five years and 63 percent of those positions have not been filled . So, it's easy to see why companies don't have the staff to check all the ways a user might attack a mainframe.

Isn't mainframe security danger just hype?

If, as Forrester states, the number of employees who can manage mainframes keeps decreasing and those positions are not being refilled, how can mainframe hacking truly be a problem? Aren't there very few people who even understand the technology? The answer to both questions is yes, which is why mainframe hacking has become a target for attackers. From a criminal's viewpoint, mainframes can be an unlocked candy shop because there have not been many IT experts worried about mainframe hacking. But just as with the x86 landscape, now attackers are publishing attack tools and papers about mainframe technologies, and the landscape is changing. Cybercrime tools and kits can be purchased for as little as $1 on the Dark Web and online marketplaces, according to the Cybersecurity Almanac 2019 by Cybersecurity Ventures . In essence, we are moving towards an attacker-rich environment from an attacker-poor environment.

Locking down the mainframe with security testing

There are a few simple steps an IT department can take to reduce the risk of a mainframe compromise:

First, and most obvious, is to make sure passwords are long and complex—a passphrase with at least 15 characters is best and should be something that the user can easily remember such as, "myc@tisnamedFluffy1." No use of "Password1," the most common password in the world.

Second, make sure users are not over-privileged. Run through your list of employees, partners, even customers who have access to your mainframe and establish a baseline of who and what should have access to your system.

Third, deploy the latest version of encryption protocols. This helps achieve the data security that's demanded from stakeholders, auditors, compliance regulations and most importantly, customers.

Fourth, consider mainframe security testing.

What about vulnerability assessments?

Unfortunately, tools for mainframe vulnerability assessments typically are not prevalent, and those that are cannot uncover undiscovered, dangerous vulnerabilities that can be exploited by a human attacker. The best course of action to identify mainframe security flaws is to perform a manual penetration test. In essence, during a penetration test, hackers try to compromise a mainframe using the same tools techniques, practices and mindset as a criminal. Once they find a flaw, they may even go a step further and use that flaw to move deeper into the target's environment. They may also chain flaws together to gain the highest level of access into the mainframe, and as such, the victim's most important data. Penetration testers look for misconfiguration issues, LPAR issues, over-privileged users, privilege escalation techniques and other undiscovered mainframe flaws. Once discovered, they can then provide remediation recommendations so that the targeted company can fix the flaws before criminal attackers can find them.

Manual penetration testing should be performed by an outside team of hackers, even if the targeted organization has conducted testing internally. Internal testers may lack a global view across many organizations of the threats to and vulnerabilities exposing mainframes; they are most likely limited to a view of only their own environment. Security leaders must also consider that someone in-house could adjust the results to make their security posture "look better" or fit together more understandably with another set of data. Finally, many compliance requirements mandate an outside independent party performs testing.

X-Force Red: Our mission—
Hacking anything to secure everything

Manual penetration tests conducted by an external team of hackers can be cost effective, especially when considering that the cost of an average data breach is $3.86 million, up 6.4 percent from last year—and that's not including the additional legal, compliance, credit monitoring and dark web monitoring fees, in addition to brand damage. Breaches also increased 2.2 percent from the previous year .

Enter X-Force® Red. X-Force Red is an autonomous team of veteran hackers, within IBM Security, hired to break into organizations and uncover risky vulnerabilities that criminal attackers may use for personal gain. X-Force Red offers penetration testing, adversary simulation and vulnerability management programs to help security leaders identify, prioritize and remediate security flaws covering their digital and physical ecosystem. With X-Force Red's attacker mentality, the team can uncover, prioritize and help fix security vulnerabilities across the IT infrastructure, doing what criminal attackers can do, with the goal of helping security leaders harden their defenses to protect their most important assets. X-Force Red's hackers are security and mainframe experts, some of whom were also mainframe administrators. The team's mainframe testing services can include:

- **Scoping.** Discovering how many mainframes and/or deployed applications a company wants tested.
- **User segment testing.** Posing as a user similar to what an attacker would do—to see if unauthorized users can gain access to and leverage mainframe session data or credentials.
- **Exploitation.** Exploiting vulnerabilities by using job control language (JCL), for example. Exploitation shows how an attacker could escalate privileges and gain further access to sensitive assets.
- **Advanced mainframe application testing.** Using a proprietary exploit tool, X-Force Red can identify if an attacker could leverage how an application is coded to break out of the application and gain access to the mainframe or escalate privileges.
- **User control testing.** Identifying if encryption is deployed on sessions, if passwords are weak, and other user-centric security controls.

All test results are available on demand, as vulnerabilities are uncovered, through the X-Force Red Portal, so that remediation may begin immediately. Once the testing is completed, X-Force Red issues a comprehensive report that includes vulnerabilities found, methodology used and remediation recommendations.

Conclusion

Mainframes are at the heart of almost every financial transaction in the United States—yet they are sometimes omitted when scoping security programs for testing. The reality is that even though mainframes are isolated with their own security controls, and there is limited mainframe hacking expertise, compromises can happen. Continuous testing services can help expose vulnerabilities criminal attackers could potentially leverage to steal sensitive corporate and customer information.

To learn more about X-Force Red Mainframe Testing and how it can help you identify potentially exploitable mainframe vulnerabilities, visit ibm.com/xforcered or talk to an IBM representative or Business Partner.

IBM Corporation Route 100
Somers, NY 10589

Produced in the United States of America, 2019

1. www.zdnet.com/article/with-the-world-embracing-cloud-computing-who-needs-mainframes
2. resources.compuware.com/forrester_mainframe_workloads_increasing_staff_losses_unfilled
3. itic-corp.com/blog/2018/08/itic-2018-server-reliability-mid-year-update-ibm-z-ibm-power-lenovo-system-x-hpe-integrity-superdome-huawei-kunlun-deliver-highest-uptime
4. ibm.com/it-infrastructure/resources/tools/server-product-comparison/#z-mainframe-product-comparison
5. blog.syncsort.com/2018/09/mainframe/mainframe-original-cloud-computing
6. enterprise.verizon.com/resources/reports/dbir
7. resources.compuware.com/forrester_mainframe_workloads_increasing_staff_losses_unfilled
8. www.thesslstore.com/blog/80-eye-opening-cyber-security-statistics-for-2019
9. 2018 Cost of a Data Breach Study: Global Overview, Benchmark research sponsored by IBM Security and independently conducted by Ponemon Institute LLC, ibm.biz/BdzKVi
10. Ibid
11. www.allerin.com/blog/why-do-banks-still-use-mainframes

A9NKZ8WE